SUSPICIOUS ACTIVITIES

It is important to always remain alert to any suspicious activities. Follow facility security procedures whenever such an event arises. When encountering a suspicious individual, make clear observations so you can record a physical description of the individual including any unique identifying features. If possible, document other pertinent information including vehicle description, license number and egress direction.

Never put yourself at risk.

Report the incident to the local law enforcement agency immediately.

Write down everything you witnessed immediately.

REPORT TO LAW ENFORCEMENT AUTHORITIES:

suspicious activities, vehicles, or persons.
break-ins.
missing chemicals, equipment, or critical blank document forms.

Employee and Contractor Security

Threats that "come from within" are the **most difficult** to detect.

Develop and implement security procedures pertaining to proper authorization for employees who work in sensitive or restricted areas.

Establish background screening policies for all employees.

Implement prohibition policies and reporting procedures for employees regarding physical violence, verbal abuse, willful destruction of property, and intimidation.

EMERGENCY CONTACTS

Maintain communication links with local and state law enforcement agencies to stay up-to-date on potential threats within your community.
Local law enforcement: _____

Local Emergency Planning Committee:
_____

FEDERAL OFFICES:

DHS (Watch & Warning Unit): 1(888) 585-9078

FBI - Boston, MA (617) 742-5533

FBI - New Haven, CT (203) 503-5000

EPA New England Environmental Emergency (NRC) (800) 424-8802

NON-EMERGENCY CONTACT INFO:

EPA New England Customer Call Center:
(888) 372-7341
(617) 918-1111

Mailing address:

EPA New England, Region 1
1 Congress Street, Suite 1100
Boston, MA 02114-2023

For additional information on chemical security, please visit EPA's web site at:
http://yosemite.epa.gov/oswer/ceppoweb.nsf/content/index.html

INDUSTRY SECURITY AWARENESS

for

Industrial Facilities
Pipelines
Transporters
Utilities
Warehousers of Chemicals

Homeland security is now one of our nation's highest priorities. We must all take part in safeguarding against terrorism.

The purpose of this bulletin is to provide security suggestions and to increase awareness on security matters that impact your facility, its productivity, and your community.

March 2003

EPA
Region 1, New England

Robert W. Varney
Regional Administrator

Management Issues

In today's society, security is everyone's responsibility. Risk-based management decisions must be made through planning:

Use a risk-based approach to assess and select the right security control measures.

Security should be given consideration as one of the company's core values. Establish written company policies and procedures pertaining to security.

Assign the oversight of security (e.g., physical, personnel, and information systems) to top managers.

Include security in all appropriate training courses.

Work with local, state, and federal law enforcement and other public safety agencies.

Be an active member of your LEPC.

Integrate site security into the facility's Emergency Response Plan.

Assess and periodically reassess facility security systems. Identify any existing or potential threats, targets, vulnerabilities, hazards, risks, as well as mitigation and countermeasures.

Consider just-on-time management of extremely hazardous substances. Keep and use the least amount of chemicals on-site as possible. Explore product substitution.

Review suppliers' transportation security procedures.

Regularly update written security policies and procedures, including the following:

physical security systems

results of vulnerability and/or risk assessment

procedures for referring suspicious incidents to appropriate authorities

protection of business information, computers, and networks

procedures for emergency response, crisis management, and shutdown

recognition of security breaches and proper actions to be taken

a system for collecting and analyzing reports of security incidents

list of contact names and information for reporting security incidents

Site Security

Are you a target for terrorism?
Physical security measures may deter such adversaries. Consider the following:

Identify facility assets that could be used as a weapon of mass destruction (**WMD**).

Establish layers of protective measures, starting at the facility's perimeter that will detect, delay and respond to security issues.

Perimeter protection measures include fences and exterior walls, bollards, trenches, personnel gates and turnstiles, vehicle gates, and security lighting.

Access control measures, such as signs, locks, alarm systems, security doors and windows, and card-based access control systems.

An integrated intrusion detection system with alarm communication and display and CCTV equipped with behavior recognition software.

Employ skilled security personnel to aid in access control and emergency response.

Protect and secure electricity, communications, and other utilities with uninterrupted and backup power source such as a generator.

Information, Computer, and Network Security

Information, computer, and network security are distinguished from physical security because information protection goes beyond proprietary information and business procedures. Potential adversaries can obtain information on chemical processes and hazardous materials from a company's computer and network systems. The following tips should be considered in establishing information security:

Use protective hardware and software.

Establish procedures for protecting and destroying sensitive documents.

Change codes and passwords following a termination of employment.

Back up all critical information and data at an alternate location.

Don't leave personal planning/scheduling devices unattended.

Be aware that sensitive information conveyed by telephone conversations, radio communications, and network communications can be intercepted. Consider using voice encryption.

Periodically analyze computer transaction histories to look for irregularities that might indicate variances in normal procedures and/or security breaches.